In.Te.S.A. S.p.A.
Qualified Trust Service Provider
ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

Manuale Operativo
per i servizi fiduciari qualificati di
Firma Elettronica, Sigillo Elettronico e Validazione Temporale Elettronica.

Codice documento: MO_QTSP

OID: 1.3.76.21.1.50.100

Redazione: Antonio Raia

Approvazione: Simone Baldini

Data emissione: 13/12/2021

Versione: 12

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A.

Revisioni

Versione n°: 12	***Data Revisione: 13/12/2021***
Descrizione modifiche:	Aggiornamento dati societari e logo Correzione refusi
Motivazioni:	Variazione proprietà, direzione e coordinamento
Versione n°: 11	***Data Revisione: 17/06/2021***
Descrizione modifiche:	Aggiornamento definizioni e riferimenti normativi Formattazione Documento - Variazione logo Inserimento riferimenti a Sigillo Elettronico Qualificato Aggiornamento par. *D - Responsabilità e limitazioni agli indennizzi* Aggiornamento par. *F - Modalità di identificazione e registrazione degli utenti* Aggiornamento par. *O - Modalità per l'apposizione e la definizione del riferimento temporale* Inserimento par. *R - Lead Time e Tabella Raci per il rilascio dei certificati* Inserimento par. *S - Riferimenti Tecnici*
Motivazioni:	Aggiornamenti normativi Variazioni operative Correzione refusi Revisione documentale
Versione n°: 10	***Data Revisione: 21/11/2016***
Descrizione modifiche:	Variazione dati societari e logo Aggiornamento definizioni e riferimenti normativi Aggiornamenti Obblighi delle LRA Esterne (C.5) Aggiornamento cap. 0 - Tariffe Inserimento procedura per Riconoscimento a Distanza Aggiornamento cap. Q - Modalità operative per la generazione della firma digitale Formattazione Documento
Motivazioni:	Aggiornamenti normativi: Regolamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 Variazioni organizzative Variazioni operative Aggiornamento tariffe Revisione documentale
Versione n°: 09	***Data Revisione: 13/06/2012***
Descrizione modifiche:	Variazione riferimenti al software di Verifica Variazione dati Amministratore Delegato Sostituzione CNIPA con DigitPA
Motivazioni:	Sostituzione del software di firma e verifica Variazioni organizzative DL 177 – 01/12/2009
Versione n°: 08	***Data Revisione: 30/11/2009***
Descrizione modifiche:	Variati i riferimenti di legge: aggiornamenti al DPCM 30/03/09 e alla Deliberazione CNIPA 21/05/2009 Cambio Amministratore delegato
Motivazioni:	Adeguamento alla nuova normativa vigente Variazioni organizzative
Versione n°: 07	***Data Revisione: 10/07/2007***
Descrizione modifiche:	1. Variato indirizzo sede 2. Variati recapiti telefonici

	3. Nel Par.A.2.Validità, aggiunta l'autorizzazione all'utilizzo delle chiavi di certificazione per la generazione e la verifica delle firme associate a certificati destinati all'autenticazione dei server 4. Nel Cap. G. Modalità di generazione delle chiavi, inserite indicazioni circa la lunghezza delle chiavi di certificazione, di validazione temporale e di sottoscrizione ***5.*** Nel Par.*H.3.1.Informazioni contenute nei certificati*, eliminato il periodo <<L'indicazione del fatto che un certificato sia qualificato è attestato dalla presenza di un'apposita estensione "*QcStatements*" (OID 1.3.6.1.5.5.7.1.3) impostata al valore "QcStatement-1".>>
Motivazioni:	Trasloco in nuova sede Precisazioni tecniche
Versione n°: 06	***Data Revisione: 30/11/2006***
Descrizione modifiche:	Introdotti i "Riferimenti di Legge" al Codice dell'Amministrazione Digitale
Motivazioni:	Adeguamento alla normativa vigente
Versione n°: 05	***Data Revisione: 22/02/2005***
Descrizione modifiche:	1. In "Riferimenti di Legge" modificato "DL 196 30/06/03" con "DLGS 196 30/06/03" 2. In "Definizioni e acronimi" aggiunte definizioni di "OID" e "ObjectIdentifier" 3. In "Riferimenti tecnici" aggiunto RFC3039 4. Nel Cap. B.1 "Dati Identificativi della versione del Manuale Operativo" aggiunto OID 5. Nel Par. H.3.1 "Informazioni contenute nei certificati" aggiunti dettagli sui contenuti dei certificati qualificati. 6. Nel Par. O "Servizio di validazione temporale" eliminato l'ultimo punto relativo alla verifica della marca temporale. 7. Aggiunto Par. O.3 "Modalità di richiesta e verifica marche temporali" 8. Nel Cap. O "Modalità per l'apposizione e la definizione del riferimento temporale" dichiarata la conformità al DPCM 13/01/04 Art.39.2. Aggiunto Par. 0 "Formati dei documenti"
Motivazioni:	Recepimento delle osservazioni di CNIPA sulla precedente versione
Versione n°: 04	***Data Revisione: 02/02/2005***
Descrizione modifiche:	1. Aggiunti capitoli: • Modalità per l'apposizione e la definizione del riferimento temporale • Modalità operative per l'utilizzo del sistema di verifica delle firme • Modalità operative per la generazione della firma digitale. 2. Sostituiti i riferimenti al DPCM 08/02/99 con riferimenti al TU e DPCM 13/01/04. 3. Modificati i dati identificativi del Certificatore nel Cap. B.2 4. Sostituiti i dati del Responsabile del Manuale Operativo nel Cap. B.3 5. Estensione dell'utilizzo delle chiavi di certificazione per l'emissione di certificati di CNS e di Crittografia Rivisto e completato il Par. I.1.3 Revoca su richiesta del Terzo Interessato
Motivazioni:	Adeguamento alla normativa vigente Aggiornamento delle procedure interne Cambiamento indirizzo sede legale dell'azienda
Versione n°: 03	***Data Revisione: 07/10/2002***
Descrizione modifiche:	Correzioni o integrazioni in: pag. 6: eliminato riferimento al DL 23/01/2002; pag. 17: integrazione al quinto elenco puntato; pag. 23: penultimo capoverso; pag. 25: terzo capoverso; pag. 27: punto "d"; pag. 34: paragrafo K.2.2 primo capoverso.
Motivazioni:	Aggiornamenti

Versione n°: 02	***Data Revisione: 20/06/2002***
Descrizione modifiche:	Aggiornamenti
Motivazioni:	Riorganizzazione aziendale; recepimento nuove normative; revisione procedure di emissione e gestione certificati; modifica URL dei servizi INTESA; aggiornamento Riferimenti di Legge; aggiornamento Definizioni e Acronimi; termini assicurativi; prezzo certificati.
Versione n°: 01	***Data Revisione: 12/10/2000***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

Revisioni **2**
Sommario **5**
Riferimenti Normativi & Acronimi **7**
Riferimenti di legge 7
Definizioni & Acronimi 7
A. Introduzione **8**
A.1. Proprietà intellettuale 9
A.2. Validità 9
B. Generalità **9**
B.1. Dati identificativi della versione del Manuale Operativo 9
B.2. Dati identificativi del QTSP – Qualified Trust Service Provider 10
B.3. Responsabilità del Manuale Operativo 10
B.4. Entità coinvolte nei processi 10
B.4.1. Certification Authority (CA) 10
B.4.2. Registration Authority (Ufficio RA) 10
B.4.3. Altre entità 11
C. Obblighi **11**
C.1. Obblighi del QTSP INTESA 12
C.2. Obblighi del Titolare 13
C.3. Obblighi degli utilizzatori dei certificati 13
C.4. Obblighi del Terzo Interessato 13
C.5. Obblighi delle LRA 14
D. Responsabilità e limitazioni agli indennizzi **15**
D.1. Responsabilità del QTSP – Limitazione agli indennizzi 15
D.2. Responsabilità finanziaria - copertura assicurativa 15
E. Tariffe **15**
F. Modalità di identificazione e registrazione degli utenti **15**
F.1. Identificazione certa iniziale del richiedente il certificato 15
F.1.1. Identificazione de visu, in presenza 16
F.1.2. Identificazione de visu, da remoto 16
F.1.3. Firma elettronica qualificata 18
F.1.4. Identità Elettroniche 18
F.1.5. Certificati di firma digitale in particolari ambiti chiusi di utenti 19
F.1.6. Identificazione tramite credenziali utilizzate per l'emissione di un precedente certificato one-shot 20
F.2. Registrazione e Richiesta di certificazione 21
F.2.1. Richiedente generico - persona fisica 21
F.2.2. Richiedente generico - persona giuridica 21
F.2.3. Contratto di servizio tra INTESA ed Ente/Azienda cliente 22
F.2.4. Limitazioni d'uso 22
F.2.5. Abilitazioni professionali e poteri di rappresentanza 22
F.2.6. Uso di pseudonimi 23
F.3. Processo di recepimento della richiesta 23
G. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione **23**
G.1. Generazione delle chiavi di certificazione 23
G.2. Generazione delle chiavi del sistema di validazione temporale 23
G.3. Generazione delle chiavi di sottoscrizione 23
H. Modalità di emissione dei certificati **24**
H.1. Procedura di emissione dei certificati di certificazione 24
H.2. Procedura di emissione dei certificati di validazione temporale 24

H.3. Procedura di emissione dei Certificati di sottoscrizione 24
H.3.1. Informazioni contenute nei certificati di sottoscrizione 25
H.3.2. Accettazione del certificato 25
I. Modalità di revoca e sospensione dei certificati 25
I.1. Revoca dei certificati 25
I.1.1. Revoca su iniziativa del Certificatore 25
I.1.2. Revoca su richiesta del Titolare 26
I.1.3. Revoca su richiesta del Terzo Interessato 26
I.2. Sospensione dei certificati 27
J. Modalità di sostituzione delle chiavi 27
J.1. Sostituzione delle chiavi del Certificatore 27
J.1.1. Sostituzione in emergenza delle chiavi di certificazione 27
J.1.2. Sostituzione pianificata delle chiavi di certificazione 27
J.1.3. Sostituzione delle chiavi del sistema di validazione temporale (TSA) 28
J.2. Sostituzione delle chiavi del Titolare 28
K. Registro dei certificati 28
K.1. Modalità di gestione del Registro dei certificati 28
K.2. Accesso logico al Registro dei certificati 28
K.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati 28
L. Modalità di protezione della riservatezza 29
M. Procedura di gestione delle copie di sicurezza 29
N. Procedura di gestione degli eventi catastrofici 29
O. Modalità per l'apposizione e la definizione del riferimento temporale 29
O.1. Controllo del sincronismo con l'ora campione 30
O.2. Timestamp token – Marca temporale 30
O.3. Modalità di richiesta e verifica marche temporali 30
P. Modalità operative per l'utilizzo del sistema di verifica della firma 30
Q. Modalità operative per la generazione della firma digitale 31
Q.1. Firma mediante dispositivo di firma individuale 31
Q.1.1. Software di firma e verifica – DigitalSign 31
Q.1.2. Software di firma e verifica – firma4ng 32
Q.2. Firma con procedure automatiche 32
Q.3. Firma Digitale Remota 32
Q.4. Firma con certificato di validità temporale limitata ("one shot") 32
Q.5. Autenticazione Biometrica 33
Q.6. Formato dei documenti 33
Q.6.1. Macroistruzioni nei documenti 33
R. Lead Time e Tabella Raci per il rilascio dei certificati 34
S. Riferimenti Tecnici 34

Riferimenti Normativi & Acronimi

Riferimenti di legge

Testo Unico - DPR 445/00 e ss.mm.ii.	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*. Nel seguito indicato anche solo come *TU*.
CAD - DLGS 82/05 e ss.mm.ii.	Decreto Legislativo 7 marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale"*. Nel seguito indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e ss.mm.ii.	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, n.d.r.).* Nel seguito indicato anche solo come *DPCM.*
Regolamento (UE)N. 910/2014 (eIDAS) e ss.mm.ii.	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS.*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) Nel seguito indicato anche solo come *GDPR.*
DETERMINAZIONE N. 147/2019 e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel seguito indicato anche solo come *DETERMINAZIONE* ovvero *LLGG*

Definizioni & Acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP Qualified Trust Service Provider. Certificatore Accreditato	*Prestatore di Servizi Fiduciari Qualificato*. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A.
Servizio Fiduciario Qualificato	Servizio elettronico fornito da un QTSP e consistente negli elementi di cui all'Art.3, punto 16) e 17) del Reg. UE 910/2014 (eIDAS). Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta i servizi qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime.
Certificato Qualificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Reg. UE 910/2014 (eIDAS)
Chiave Privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave Pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale sul documento informatico.
CRL	Lista dei Certificati Revocati, Certificate Revocation List, un elenco che riporta i certificati revocati o sospesi, non più considerati validi dal Certificatore che li ha emessi.

OCSP	Online Certificate Status Protocol: servizio di verifica dello stato di validità del Certificato, secondo il protocollo OCSP.
Documento informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Firma elettronica creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
Firma Remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
HSM - Hardware Security Module	Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014. Anche detti *Dispositivi di Firma*.
Qualified Electronic Time Stamp *(Marca Temporale)*	*Validazione Temporale Elettronica Qualificata* Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi dati esistevano in quel momento. Risponde ai requisiti dell'Art.42 del Reg. eIDAS
CA - Certification Authority	Autorità che emette i certificati per la firma elettronica.
RA - Registration Authority	*Autorità di Registrazione*: entità che, su incarico del QTSP, ha la responsabilità di registrare e verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al QTSP per emettere il Certificato Qualificato.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Richiedente *Richiesta di certificazione*	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione.
Titolare	La Persona Fisica cui il certificato qualificato di firma è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma digitale.
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
TSA - Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
Giornale di Controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il QTSP, tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza (DPCM 22/02/2013, Art. 36
CPS - CP	*CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico* del QTSP INTESA: documento costituisce il Practice Statement del QTSP e descrive le regole e le procedure operative per l'emissione dei certificati qualificati di firma elettronica e di sigillo elettronico, come definiti nel Regolamento (UE) 910/2014 (eIDAS). E' pubblicato sul sito dell'Agenzia e dal QTSP all'URL: *https://www.intesa.it/e-trustcom/*

A. Introduzione

Il presente documento è il Manuale Operativo per i servizi qualificati di Firma elettronica, Sigillo elettronico e Validazione temporale elettronica forniti da *In.Te.S.A. S.p.A. (a Kyndryl Company)*.

Il Manuale Operativo descrive le procedure e relative regole utilizzate dal *Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A.* (di seguito anche solo *QTSP INTESA, Certificatore Accreditato* o *INTESA*) per l'emissione dei Certificati Qualificati per la Firma Elettronica e per il Sigillo Elettronico, e per l'emissione delle Validazioni temporali elettroniche qualificate (dette anche *marche temporali* o *Time Stamp*).

Il contenuto di questo Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel *Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013* (di seguito *DPCM*) e dal *D. lgs. 7 marzo*

2005, n. 82, recante il "Codice dell'Amministrazione Digitale" come successivamente modificato e integrato (di seguito "*CAD*") ed è conforme al *Regolamento UE 910/2014* (nel seguito, *Reg. eIDAS*).

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme vigenti e future che regolano la fattispecie concreta.

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS).

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di Prestatore di servizi fiduciari è coperto da diritti sulla proprietà intellettuale.

A.2. Validità

Quanto descritto in questo documento si applica al TSP INTESA, cioè alle sue infrastrutture logistiche e tecniche, al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma digitale relativa ad essi, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 del DPCM, che, al comma 4, distingue le chiavi e i correlati servizi secondo le seguenti tipologie:
chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati e alle loro liste di revoca (CRL) o sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali;
chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati (OCSP);
chiavi destinate alla sottoscrizione del separato certificato di attributo.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e relative regole utilizzate dal QTSP INTESA per l'emissione di certificati qualificati ai sensi del Reg. eIDAS.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei Certificatori accreditati tenuto da AgID.

Pertanto, in funzione delle normative menzionate, vengono coinvolte più entità che saranno meglio identificate nel proseguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n. ***12*** del ***Manuale Operativo per i servizi fiduciari qualificati di Firma Elettronica, Sigillo Elettronico e Validazione Temporale Elettronica***, rilasciata il ***13/12/2021*** in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.50.100***.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica:

- all'indirizzo Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*

Nota: la pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire solo previa autorizzazione dell'Agenzia per l'Italia Digitale.

B.2. Dati identificativi del QTSP – Qualified Trust Service Provider

Il QTSP (*Prestatore di Servizi Fiduciari Qualificato*) è la società ***In.Te.S.A. S.p.A.***, di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	*In.Te.S.A. S.p.A.*
Indirizzo della sede legale	*Strada Pianezza, 289* *10151 Torino*
Legale Rappresentante	*Amministratore Delegato*
Registro delle Imprese di Torino	*N. Iscrizione 1692/87*
N. di Partita I.V.A.	*05262890014*
N. di telefono (centralino)	*+39.011.19216.111*
Sito Internet	*www.intesa.it*
Indirizzo di posta elettronica	*marketing@intesa.it*
Indirizzo (URL) registro dei certificati	*ldap://x500.e-trustcom.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21*

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art.40 comma 3 lett. c) del DPCM, è del QTSP INTESA, che ne cura la stesura e la pubblicazione.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, il QTSP INTESA ha predisposto i seguenti strumenti:

- un recapito di posta elettronica *uff_RA@intesa.it*
- un recapito telefonico: *+39.011.19216.111*
- un servizio di Help Desk *www.hda.intesa.it*
  - *per le chiamate dall'Italia* *800.80.50.93*
  - *per le chiamate dall'estero* *+39 02.39.30.90.66*

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal QTSP espletando, per la parte di loro competenza, le attività a loro attribuite.

B.4.1. Certification Authority (CA)

INTESA, operando in ottemperanza a quanto previsto dal DPCM, dal CAD e dal Reg. eIDAS, espleta le attività di Qualified Trust Service Provider. Tali attività includono i servizi fiduciari qualificati di creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche (marche temporali).

I dati identificativi del QTSP INTESA sono riportati al precedente paragrafo B.2.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti:

a) Responsabile della sicurezza.
b) Responsabile del servizio di certificazione e validazione temporale.
c) Responsabile della conduzione tecnica dei sistemi.
d) Responsabile dei servizi tecnici e logistici.
e) Responsabile delle verifiche e delle ispezioni (auditing).

Le figure sopra elencate sono tutte appartenenti all'organizzazione del QTSP INTESA.

B.4.2. Registration Authority (Ufficio RA)

INTESA ha costituito al suo interno un'entità denominata *Ufficio RA* che ha funzioni di Registration Authority.

In particolare, essa espleta le seguenti attività:

- Identificazione dei titolari.
- Registrazione dei titolari.
- Inizializzazione dei dispositivi di firma.
- Distribuzione dei dispositivi di firma.
- Gestione dell'inventario dei dispositivi di firma.
- Supporto al Titolare.

L'Ufficio RA, all'interno di specifici accordi, ha inoltre l'incarico d'istruire il personale di entità esterne per la costituzione di *Local Registration Authority (LRA)*. Queste ultime operano sul territorio svolgendo, anche solo in parte, le attività sopra elencate su incarico di INTESA.

Il QTSP INTESA può inoltre demandare lo svolgimento di alcune funzioni della propria RA ad entità esterne (par. B.4.3.4) vedi . Nel Contratto di Mandato, sottoscritto da entrambe le parti, saranno definite le attività in carico alla LRA esterne e riportati gli obblighi delle parti.

La RA INTESA e le LRA sono oggetto di audit e vigilanza da parte del QTSP, al fine di verificare il rispetto della normativa vigente.

B.4.3. Altre entità

B.4.3.1. Titolare del certificato qualificato

Persona fisica o giuridica cui è attribuita la firma elettronica o il sigillo elettronico, che ha accesso ai dispositivi per la creazione della firma elettronica o del sigillo elettronico.

È il soggetto intestatario del certificato.

B.4.3.2. Terzo interessato

Il Terzo Interessato è la persona fisica o giuridica (impresa, associazione di categoria, ente, ecc.) che richiede o autorizza l'emissione del certificato qualificato. Ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato.

B.4.3.3. Utilizzatore (Relying Party)

L'Utilizzatore è colui che, verificando il documento elettronico, utilizza i certificati (e le eventuali marche temporali) emesse dal QTSP INTESA.

B.4.3.4. LRA – Local Registration Authority

Il QTSP INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale, ai sensi dell'art. 1703 del codice civile, di ulteriori soggetti (nel seguito denominati LRA esterne) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. .In particolare, le LRA esterne espletano le seguenti funzioni:

- identificazione certa del titolare del certificato;
- raccolta della richiesta di registrazione e certificazione compilata e sottoscritta dal Titolare;
- consegna del dispositivo di firma e/o delle credenziali per il controllo esclusivo della chiave privata

La documentazione raccolta deve essere trasmessa all'Ufficio RA di INTESA ovvero, previo accordo, trattenuta e conservata dalla LRA con le stesse modalità.

Le LRA esterne sono attivate dal QTSP a seguito di un adeguato addestramento del personale indicato dall'Azienda o Ente con il quale viene stipulato un regolare Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere l'Azienda o Ente cui INTESA assegna l'incarico di LRA (vedi par. *C.5 - Obblighi delle LRA*).

C. Obblighi

Nel seguito sono riportati gli obblighi cui devono sottostare i partecipanti alla PKI (par. *B.4 - Entità coinvolte nei processi*).

C.1. Obblighi del QTSP INTESA

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche (CAD)
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013 (DPCM)
- Regolamento (UE) 2016/679 (GDPR)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il QTSP INTESA:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione di firme e/o sigilli (HSM) abbia i requisiti di sicurezza previsti del Reg. eIDAS (artt. 29 e 39);
- identifica con certezza il richiedente la certificazione (futuro Titolare del certificato);
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'art. 32 del CAD;
- informa i richiedenti, in modo esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni, in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza di INTESA) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione;
- fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali (DPCM, Art.14).
- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati ai sensi dell'art. 42 del DPCM;
- mantiene copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di certificazione di cui all'art. 43 del DPCM, e la rende accessibile per via telematica come stabilito dall'art. 42, comma 3 del DPCM;

- conduce periodicamente verifiche e ispezioni (audit) al fine di vigilare sulle attività delle LRA, riservandosi il diritto di interrompere il servizio qualora, a seguito dei predetti audit, emergesse che le attività di identificazione non venissero espletate in maniera idonea e conforme al Manuale Operativo, al CPS e alle normative vigenti.

C.2. Obblighi del Titolare

Il Titolare al quale è stato attribuito un certificato qualificato per i servizi fiduciari del QTSP INTESA, oggetto nel presente Manuale Operativo, è tenuto a conservare le informazioni necessarie all'utilizzo della propria chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, art. 32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone la correttezza e completezza sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo CPS e nel MO di riferimento;
- comunicare al QTSP INTESA, anche per tramite della LRA, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente CPS;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (art. 5, comma 5, del DPCM);
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma;
- revocare o sospendere il certificato digitale secondo quanto indicato nel presente CPS e nel MO di riferimento.

C.3. Obblighi degli utilizzatori dei certificati

L'Utilizzatore (*Relying Party*) è chiunque riceva un documento firmato digitalmente e, al fine di verificarne la validità, si avvalga del certificato qualificato utilizzato dal Titolare per firmare il documento stesso.

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in conformità al Reg. eIDAS.

Coloro che si avvalgono di un certificato qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato dagli standard vigenti al momento della sua emissione;
- verificare lo stato di validità del certificato mediante il protocollo OCSP o tramite l'accesso alle Liste di Revoca;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei QTSP;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, nei servizi oggetto del presente CPS, è tipicamente l'organizzazione (cliente) che stipula un contratto di fornitura di servizi fiduciari con il QTSP.

Il Terzo Interessato:

- autorizza formalmente il QTSP all'utilizzo del campo *organizationName* del certificato;
- verifica che il Titolare sia in possesso di tutti i requisiti necessari e autorizza il medesimo a richiedere il rilascio del certificato qualificato di firma elettronica;
- indica al QTSP INTESA eventuali ulteriori limitazioni d'uso del certificato qualificato;
- indica al QTSP INTESA eventuali titoli o poteri di rappresentanza del Titolare;

Il Terzo Interessato si assume l'obbligo di richiedere la revoca del certificato nel caso in cui il titolare del certificato lasci l'organizzazione ovvero vengano meno i requisiti per cui è stato richiesto il certificato (ad es. subentri una variazione o cessazione dei poteri di rappresentanza).

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente comunicata al QTSP quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato un certificato qualificato per la firma elettronica.

Il terzo interessato dovrà altresì comunicare ogni variazione dei dati identificativi dell'azienda (es. denominazione sociale, sede legale, etc.), cessazione dell'attività da parte dell'organizzazione e ogni altro dato rilevante o che influisca ai fini dell'uso del certificato.

C.5. Obblighi delle LRA

INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale di ulteriori soggetti (nel seguito, *LRA – Local Registration Authority*) per svolgere una parte delle attività proprie dell'Ufficio di registrazione.

Tipicamente, una LRA è demandata ad espletare le seguenti attività:

- identificazione certa del richiedente la certificazione (titolare del certificato);
- registrazione del richiedente / Titolare;
- consegna ai Titolari dei dispositivi di firma individuale (smartcard / token usb)
- consegna al Titolare dei codici che gli permetteranno di accedere alla propria chiave di firma nel rispetto degli artt. 8 e 10 comma 2 del DPCM;
- invio della documentazione sottoscritta all'Ufficio RA di INTESA, salvo differenti accordi riportati sul contratto di mandato.

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere la LRA e sui quali INTESA ha l'obbligo di vigilare.

In particolare, si richiede alla LRA di:

- vigilare affinché l'attività di identificazione posta in essere si svolga nel rispetto della normativa vigente (CAD, DPCM, Reg. eIDAS ed eventualmente la normativa in materia di Antiriciclaggio);
- utilizzare e trattare i dati personali acquisiti in fase di identificazione in accordo con il GDPR;
- rendere disponibile ad INTESA il materiale raccolto nella fase di identificazione e registrazione.
- conservare in modo sicuro la documentazione raccolta nella fase di identificazione e registrazione, quindi inviarla all'Ufficio RA del QTSP INTESA ovvero custodirla per 20 (venti) anni, a seconda degli accordi definiti nel contratto di mandato;
- custodire in modo sicuro i dispositivi di firma e/o le credenziali per il controllo esclusivo della chiave privata fino alla consegna degli stessi ai titolari destinatari, rispondendo direttamente della loro sottrazione o perdita per qualsiasi causa, con obbligo di comunicare senza ritardo tali eventi all'Ufficio di Registrazione di INTESA;
- impedire ai propri dipendenti la prosecuzione dell'attività di identificazione certa e curare l'immediato ritiro di ogni materiale a tal fine utilizzato, qualora, per qualsiasi causa, si interrompa il rapporto in essere tra la LRA incaricata e il dipendente stesso;
- fornire ad Intesa, in caso di verifiche ispettive o contenziosi, tutta la documentazione acquisita e sottoscritta dal Titolare all'atto del rilascio del certificato o durante il ciclo di vita del certificato, secondo quanto previsto dal Contratto e dal Manuale Operativo;
- consentire l'accesso presso i propri locali di personale del QTSP, ovvero di terzi dallo stesso incaricati, per adempiere agli obblighi di ispezione (audit); tale accesso deve essere consentito anche agli auditor incaricati dall'Organismo di Vigilanza (AgID);
- segnalare senza indugio al QTSP INTESA, per tramite dell'Ufficio RA (*uff_ra@intesa.it*) ovvero dei propri riferimenti INTESA, ogni evento o incidente inerente i punti indicati precedentemente, nonché tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi oggetto del presente CPS e del Manuale Operativo di riferimento ovvero sui dati personali dei titolari.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

Il QTSP INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, art. 13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'art. 5 del DPCM, e in particolare dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo, nel CPS e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Parimenti, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

INTESA non sarà responsabile per i danni derivanti da un utilizzo non conforme del certificato qualificato in relazione alla limitazione d'uso specificata sul certificato stesso.

Il Titolare, a seguito della presa visione del Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal QTSP.

Se non altrimenti specificata, la limitazione di responsabilità è riportata nelle *Condizioni Generali di Contratto INTESA* (www.intesa.it).

D.2. Responsabilità finanziaria - copertura assicurativa

Oltre a soddisfare il requisito minimo richiesto sul capitale sociale, INTESA è beneficiaria di contratti assicurativi per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tali contratti è resa disponibile ad AgID apposita dichiarazione di stipula.

E. Tariffe

Le tariffe per il servizio di certificazione e di validazione temporale sono pubblicate sul sito del QTSP.

Per progetti specifici, le tariffe sono concordate a livello contrattuale con il singolo cliente.

L'accesso alle informazioni riguardanti lo stato del certificato (CRL e OCSP) è libero e gratuito.

Il QTSP mette a disposizione un software di verifica a titolo gratuito (https://www.intesa.it/e-trustcom/).

Per ulteriori informazioni: ***marketing@intesa.it***

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione certa iniziale del richiedente il certificato

Il QTSP verifica con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

L'attività di identificazione del richiedente viene effettuata da:

- Il QTSP, tramite le persone del proprio Ufficio RA ovvero proprio personale adeguatamente formato;
- LRA esterne: ad esempio il personale dell'Azienda o dell'Ente Cliente oppure di terze parti appositamente delegate dal QTSP e adeguatamente formato.

La persona che fa richiesta della certificazione viene identificata con certezza dall'operatore di RA / LRA e viene archiviata dal QTSP, INTESA (o dalla LRA incaricata) copia di almeno un documento ufficiale di identità per lo Stato di appartenenza.

Se il titolare del certificato sarà una persona giuridica, la richiesta di certificazione dovrà essere avanzata dalla persona fisica che rappresenta la persona giuridica, fornendo opportuna documentazione aggiuntiva atta alla verifica dei poteri di rappresentanza (es. visura camerale). Tipicamente, il richiedente potrà essere il Legale Rappresentante, o persona da questo formalmente delegato.

La verifica certa dell'identità del Titolare può essere effettuata nelle seguenti modalità:

- *De visu, in presenza*: per l'identificazione è necessaria la presenza fisica del richiedente davanti all'operatore di RA
- *De visu, da remoto*: l'identificazione è effettuata mediante un sistema di videoconferenza con caratteristiche di qualità certificate da un *CAB* (organismo di valutazione della conformità)
- *Firma Elettronica Qualificata*, precedentemente rilasciata, anche da altro QTSP
- *Altre modalità*, purché conformi all'art. 24, comma 1, del Reg. eIDAS

Ulteriori dettagli sulle procedure di identificazione del Titolare attualmente poste in essere sono reperibili sui Manuali Operativi specifici del QTSP, pubblicati al seguente link:

- *https://www.intesa.it/e-trustcom/*

F.1.1. Identificazione de visu, in presenza

L'identificazione è operata mediante la presenza concreta della persona fisica (per i certificati qualificati di firma elettronica) o della persona fisica rappresentante la persona giuridica (per i certificati qualificati di sigillo elettronico).

F.1.2. Identificazione de visu, da remoto

Nel rispetto delle normative vigenti, il riconoscimento del Titolare può essere eseguito attraverso una procedura di identificazione remota tramite webcam, in modalità assistita con operatore ovvero, in alternativa, in modalità video self.

Il servizio consente al cliente di collegarsi nel momento a lui più comodo senza necessariamente doversi spostare dal luogo in cui si trova per eseguire tale procedura.

F.1.2.1. Video identificazione con operatore

Questa modalità prevede un'interazione tra richiedente e operatore completamente «online» e assistita, favorendo l'esperienza d'uso ed agevolando tutti coloro meno consoni all'uso delle tecnologie.

A fronte della conferma da parte dell'operatore di avvenuta identificazione, il video viene cifrato e inviato in Conservazione a Norma.

Il servizio di identificazione remota potrà essere gestito come segue:

- Il Richiedente, in possesso di un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante, si connette al sito della Registration Authority (RA) dove sono riportate tutte le istruzioni necessarie per eseguire i passi successivi e dove sono indicati i documenti necessari per l'identificazione.
- Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di RA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.
- Il Richiedente compila sul sito della RA/LRA una richiesta di certificato digitale compilando un form in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione.
- Compilato tale form, viene richiesto al Richiedente di prendere visione del presente *Manuale Operativo*, che dovrà essere aperto in lettura. Lo stesso Manuale Operativo sarà anche agevolmente scaricabile dal sito stesso.
- Fra le operazioni che necessariamente il Richiedente dovrà svolgere vi è anche l'autorizzazione al trattamento dei propri dati personali (GDPR, art. 13).
- Il Richiedente, sempre grazie alle funzionalità esposte sul sito, una volta presa visione del Manuale Operativo e dato il consenso, dovrà inviare alla RA una copia scansionata dei documenti di identità (carta d'identità, passaporto, tesserino sanitario nazionale). L'invio preventivo di tali documenti conferma la volontà del Richiedente di completare la procedura di identificazione finalizzata all'emissione di un certificato qualificato utilizzabile esclusivamente nell'ambito dei servizi di firma qualificata forniti dal TSP.

- Completata la fase di inserimento dati e invio (upload) dei documenti necessari per l'identificazione, il Richiedente potrà continuare la sessione attivando appena possibile il collegamento via webcam oppure fissando un successivo appuntamento con gli operatori di RA per completare in un momento successivo a lui più comodo la procedura.
- Gli operatori di RA, sulla base dei documenti ricevuti, possono eseguire ulteriori controlli utilizzando specifiche banche dati, come SCIPAFI (il Sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento: attualmente quelle dell'Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei Trasporti, INPS e INAIL), oppure altre banche dati private (ad es. CRIF, Cerved, ecc.) in grado di erogare servizi di verifica dati e documenti d'identità.
- Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie circa il certificato qualificato di che sta per essergli emesso.
- Durante la sessione on-line (via webcam), l'operatore di RA domanda al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi, verificando che nella foto del documento sia riconoscibile il Richiedente. Inoltre, chiede al soggetto di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del richiedente.
- L'intera sessione viene registrata in modalità audio e video (sia lato Richiedente che lato operatore) e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.
- La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa distinguibile del documento di riconoscimento inquadrato). L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione. L'operatore deve essere libero di rifiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.

La documentazione precedentemente citata, relativa alla registrazione dei Titolari, viene conservata dal QTSP INTESA per 20 (venti) anni.

F.1.2.2. Video identificazione in modalità self & welcome call

In alternativa al video riconoscimento descritto al paragrafo precedente, una possibile modalità di video identificazione è rappresentata dalla modalità "*self + welcome call*".

Il processo prevede che l'utente, in fase di identificazione, venga guidato dal sistema ad eseguire una serie di passi all'interno di una sessione video registrata.

Al richiedente sarà richiesto di:

- caricare o fotografare il proprio documento d'identità per acquisizione (dati anagrafici e foto);
- inserire il proprio codice fiscale o, eventualmente, caricare/fotografare il proprio tesserino sanitario o tesserino del codice fiscale attualmente rilasciato;
- verificare l'indirizzo di posta elettronica e il numero di cellulare tramite OTP e/o Magic Link;
- riprendere il proprio volto tramite un *video selfie* (per confronto biometrico), eseguendo contestualmente alcune azioni casuali guidate del volto guidate verifica del *liveness*. Lo stream sarà successivamente analizzato utilizzando algoritmi di riconoscimento facciale per rilevare i movimenti del viso.

Il processo di verifica potrà avvenire in automatico, attraverso un algoritmo di *Face Recognition*, per match biometrico tra foto del documento di identità e ripresa del volto (tramite alcuni fotogrammi).

In modalità *unattended* per il richiedente, vengono quindi eseguite una serie di verifiche tra cui:

- controllo sui dati anagrafici;
- verifica di leggibilità delle foto dei documenti d'identità e confronto tra fotogrammi del Video Self e la foto sul documento di identità;
- confronto tra i dati inseriti nel portale e quelli riportati nei documenti d'identità caricati;
- verifica della liveness;

- verifica con fonte autoritativa (Scipafi).

In caso di esito positivo, il video sarà accettato dal sistema, altrimenti si inviterà l'utente ad effettuare la video identificazione con operatore e il video sarà cancellato.

In caso di positivo riscontro dei controlli suindicati, un operatore autorizzato verificherà i dati del richiedente relativi ai video accettati dal sistema e confermerà il riconoscimento solo dopo aver effettuato una procedura di *welcome call*, nella quale chiederà al titolare di confermare i suoi dati e la volontà di richiedere un certificato qualificato.

Il video sarà cifrato e memorizzato su sistemi del QTPS INTESA insieme alla registrazione della welcome call.

La procedura di welcome call, necessaria ai fini dell'identificazione certa del Titolare, si compone dei seguenti step:

- Le informazioni raccolte dal Portale e dall'applicazione sono passate al backoffice e al Service Telefonico, per il completamento del riconoscimento.
- Il Cliente è quindi chiamato dal Service Telefonico (*Welcome Call*) per una verifica incrociata dell'identità: saranno poste in questa fase al cliente una serie di domande per verificare la corrispondenza tra risposte fornite e i dati/documenti acquisiti con il Self ID.

Allo scopo di assicurare la conformità del procedimento a quanto disposto dalle normative vigenti che regolano la materia, la chiamata sarà registrata e conservata per il periodo previsto di 20 (venti)) anni. La registrazione della welcome call potrà essere utilizzata quale ulteriore evidenza atta a confermare l'identità della persona e la sua volontà a procedere con la richiesta di un certificato qualificato.

F.1.3. Firma elettronica qualificata

Se il richiedente è in possesso di un certificato qualificato a lui intestato, può utilizzare la propria firma elettronica qualificata per sottoscrivere la richiesta di certificazione ed espletare così il processo di identificazione sfruttando il riconoscimento effettuato dal QTSP che ha rilasciato il suddetto certificato.

F.1.4. Identità Elettroniche

F.1.4.1. SPID

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, Il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione SPID con credenziali di livello 2 o 3.

In tale processo di autenticazione, sono richiesti i seguenti dati minimi:

- Nome
- Cognome
- Sesso
- Luogo di nascita
- Data di nascita
- Codice fiscale.

Il certificato qualificato rilasciato tramite identità digitale SPID conterrà l'***OID 1.3.76.16.5***, registrato a cura dell'Agenzia con la seguente descrizione: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*";

Eventuali certificati qualificati emessi a seguito di una richiesta sottoscritta con firma elettronica qualificata basata su tali certificati qualificati devono, a loro volta, contenente il suddetto OID.

F.1.4.2. Identificazione tramite CIE (Carta di Identità Elettronica)

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, Il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione CIE.

In questo caso il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server. Il sistema, dopo aver completato l'autenticazione, verifica le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione oggetto di richiesta.

F.1.5. Certificati di firma digitale in particolari ambiti chiusi di utenti

È possibile l'emissione di un certificato qualificato di firma elettronica prima che sia conclusa l'identificazione del Titolare solamente nel caso sussistano particolari circostanze riconducibili a limitati utilizzi della firma digitale in contesti chiusi di utenti che non consentono alle firme digitali generate di produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non termini con esito positivo.

Questa possibilità è stata confermata dall'Agenzia con la comunicazione alle CA del 7 giugno 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", avente per oggetto "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*".

Tipico è il caso in cui l'oggetto della sottoscrizione è un atto per cui sia prescritta la sottoscrizione di due o più parti, senza le quali è giuridicamente *imperfetto*, privo quindi di qualunque effetto giuridico (ad es. la richiesta di adesione a specifici servizi, quali carte di credito, conti deposito, servizi di fonia, etc..).

Gli attori sono quindi:

- Il Titolare del certificato
- Il cointeressato e cofirmatario

Il processo, conforme alla comunicazione sopra menzionata, ha le seguenti restrizioni:

1) Il processo è riconducibile esclusivamente a sistemi di firma remota;
2) L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;
3) Nel certificato qualificato del Titolare sono presenti stringenti limiti d'uso afferenti il rapporto specifico tra il Titolare e il cointeressato e cofirmatario (par. *F.1.5.1*);
4) Con l'obiettivo di distinguere chiaramente questi certificati da quelli emessi con procedure più tradizionali, il certificato qualificato del Titolare contiene uno specifico OID (par.*F.1.5.2*);
5) L'applicazione di firma remota utilizzata limita gli oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario. I documenti oggetto della sottoscrizione devono essere giuridicamente imperfetti, cioè privi di effetto fino all'apposizione della firma del cointeressato e cofirmatario. A titolo di esempio, si citano i contratti per l'adesione ad un servizio;
6) Nel caso in cui la verifica dell'identità del Titolare avvenga per mezzo di un incontro fisico fra Titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del Certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario se diverso dal Certificatore;
7) Il cointeressato e cofirmatario può espletare la verifica dell'identità, in vece del Certificatore, attraverso sessioni audio-video, attraverso le procedure indicate dal certificatore e approvate dall'AgID, ovvero in applicazione della normativa afferente la verifica dell'identità di cui al *D.lgs. 231/2007*, ove applicabile, ovvero in applicazione della normativa afferente la verifica dell'identità ai sensi della Direttiva (UE) 2018/843 e relative implementazioni a livello di singoli Stati Membro. Qualora, nell'ambito della verifica ai sensi di tale D.lgs. sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;
8) All'apposizione della firma del Titolare non viene apposta la marca temporale: che deve essere apposta obbligatoriamente dopo la firma del cointeressato e cofirmatario che rende l'atto giuridicamente perfetto;
9) Fino all'apposizione della firma e della marca di cui al precedente punto 8, l'oggetto sottoscritto dal solo Titolare non è fornito ad alcuno e, qualora la verifica dell'identità del Titolare non avesse buon fine, il documento è distrutto conservando traccia degli eventi in appositi log.

F.1.5.1. Limite d'uso specifico

Per ottemperare al punto 3) del par. *F.1.5*, sarà definito un limite d'uso specifico per questa tipologia di certificati.

Di seguito, è riportata una formula standard, a titolo di esempio:

> *"Il presente Certificato Qualificato è valido solo per la sottoscrizione di documenti relativi all'adesione ai servizi di Nome servizio erogati da Nome Azienda ai propri Clienti."*
> *"This Qualified Certificate is valid only for electronic signatures affixed to documentation relating to Nome servizio provided by Nome Azienda to its Customers."*

Specifici limiti d'uso potranno essere concordati per meglio descrivere delimitare l'abito di applicazione.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.1.5.2. OID specifico

Per ottemperare al punto 4) del par. F.1.5, il certificato emesso sotto queste condizioni è distinguibile dagli altri certificati in quanto contiene, nel campo *certificatePolicies* (OID 2.5.29.32), uno dei seguenti OID (ognuno definito in riferimento alla CA di root che ha emesso il certificato):

- ***1.3.76.21.1.3.1.1.1***
- ***1.3.76.21.1.5.1.1.1***
- ***1.3.76.21.10.2.1.2.1***

Per ulteriori approfondimenti sugli OID utilizzati dal QTSP, è disponibile il documento *CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico*, pubblicato all'URL https://www.intesa.it/e-trustcom/.

F.1.6. Identificazione tramite credenziali utilizzate per l'emissione di un precedente certificato one-shot

In questa modalità, il Certificatore si basa sull'identificazione già effettuata durante l'emissione di un precedente certificato one-shot.

Possono essere individuati due tipi di casistiche:

a) Il certificato one-shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso nell'ambito della stessa sessione o processo di firma in cui è stato rilasciato il precedente certificato one-shot.
b) Il certificato one shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso in una differente sessione o processo di firma.

Nel caso a): il Richiedente, in possesso dell'e-mail e del numero di cellulare certificati dal Certificatore nel corso del rilascio del precedente certificato one shot, può richiedere il rilascio del nuovo certificato one-shot solo dopo aver ricevuto, sull'e-mail e sul cellulare certificati, i nuovi codici One-Time, che dovranno essere verificati dal Richiedente per l'emissione e per l'utilizzo del nuovo certificato, purché ciò avvenga all'interno della stessa sessione o processo di firma.

Nel caso b): il Richiedente, già in possesso di credenziali fornite dal Certificatore o dalla LRA, si autentica al portale del Certificatore o della LRA e chiede l'emissione di un nuovo certificato one-shot, previa la conferma o l'aggiornamento dei dati di registrazione. E-mail e cellulare precedentemente certificati non potranno essere variati. In questo caso, per il rilascio e l'utilizzo del certificato è necessario che il Titolare inserisca la One-Time-Password inviata al suo dispositivo OTP, ovvero OTP/SMS su cellulare, e che sia data l'autorizzazione a procedere dalla LRA o dal Terzo Interessato.

In entrambi i casi, la gestione del sistema di autenticazione OTP è sotto il controllo della CA.

Qualora il Certificatore, durante il processo di emissione del precedente certificato one-shot, abbia certificato il possesso di strumenti di *Strong Customer Authentication* (*SCA*) riconducibili allo specifico Richiedente, tali credenziali SCA potranno essere utilizzate in luogo dei codici One-Time inviati su e-mail e cellulare nel *caso a)*, ovvero dell'accesso all'area riservata e invio di OTP/SMS nel *caso b)*.

F.1.6.1. Limiti d'uso

A maggior tutela del Richiedente, per il certificato qualificato sarà definito un limite d'uso specifico per questa tipologia di certificati.

Di seguito, è riportata una formula standard, a titolo di esempio:

> *"Il presente Certificato Qualificato è valido solo per la sottoscrizione di documenti relativi all'adesione ai servizi di Nome servizio erogati da Nome Azienda ai propri Clienti."*
> *"This Qualified Certificate is valid only for electronic signatures affixed to documentation relating to Nome servizio provided by Nome Azienda to its Customers."*

Specifici limiti d'uso potranno essere concordati per meglio descrivere delimitare l'abito di applicazione nel dominio della specifica LRA.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.2. Registrazione e Richiesta di certificazione

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi del TSP. Questa operazione viene sempre eseguita dal personale dell'Ufficio RA di INTESA, al netto di identificazioni di tipo unattended (es. Identità Elettroniche, par. *F.1.4*).

Durante la registrazione dei dati del Titolare viene generato l'identificativo univoco del Titolare presso il TSP.

F.2.1. Richiedente generico - persona fisica

Il richiedente, cioè la *persona fisica* che sarà il *Titolare* del certificato, sottoscrive:

- Il contratto di adesione al servizio, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Qualificato P.F.*, in cui riporta i dati necessari all'emissione del certificato, tra cui:
  - Cognome e nome.
  - Data e luogo di nascita.
  - Codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di C.F. italiano).
  - Numero di telefono cellulare.
  - Indirizzo di posta elettronica.
  - Tipo, numero, ente di rilascio e data di scadenza del documento di identità esibito.
- Il documento *Presa visione del Manuale Operativo INTESA*, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del GDPR.

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il QTSP (che non verifica la validità dell'indirizzo) userà in seguito tale indirizzo per comunicare con il richiedente.

La documentazione precedentemente descritta, relativa alla registrazione dei titolari, viene conservata dal QTSP (ovvero dalla LRA incaricata, se previsto dal contratto di mandato) per 20 (venti) anni dalla scadenza del certificato.

F.2.2. Richiedente generico - persona giuridica

Il richiedente, cioè la persona fisica rappresentante la *persona giuridica* che sarà il *Titolare* del certificato, sottoscrive:

- Il contratto di adesione al servizio, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Qualificato P.G.*, in cui riporta i dati necessari all'emissione del certificato, tra cui:
  - Dati anagrafici del Richiedente (Legale Rappresentante o soggetto delegato):
    - Cognome e nome.
    - Data e luogo di nascita.
    - Codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di C.F. italiano).
    - Tipo, numero, ente di rilascio e data di scadenza del documento di identità esibito.
    - Numero di telefono cellulare.
    - Indirizzo di posta elettronica.
  - Dati del Titolare (Persona Giuridica):
    - Denominazione della persona giuridica.
    - Sede della persona giuridica.
    - P.IVA o Codice Fiscale (VAT o analogo per organizzazioni con sede all'estero).
- Il documento *Presa visione del Manuale Operativo INTESA*, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del GDPR.

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il QTSP (che non verifica la validità dell'indirizzo) userà in seguito tale indirizzo per comunicare con il richiedente.

La documentazione precedentemente descritta, relativa alla registrazione dei titolari, viene conservata dal QTSP (ovvero dalla LRA incaricata, se previsto dal contratto di mandato) per 20 (venti) anni dalla scadenza del certificato.

F.2.3. Contratto di servizio tra INTESA ed Ente/Azienda cliente

Nel caso in cui il cliente sia un Ente o un'Azienda, i cui dati identificativi saranno definiti a contratto, si applicano anche le norme seguenti, fermo restando quanto specificato al par. F per l'identificazione e la registrazione dei singoli titolari:

- Le persone delegate a indicare il personale del Cliente abilitato ad essere certificato da INTESA faranno pervenire al Certificatore gli elenchi delle persone alle quali INTESA sarà autorizzata a rilasciare i certificati qualificati. In tali elenchi sarà possibile anche indicare eventuali limitazioni all'uso delle coppie di chiavi, poteri di rappresentanza o abilitazioni professionali.
- Questi elenchi saranno resi disponibili agli addetti interessati: il personale dell'Ufficio RA ovvero della LRA.
- Le persone autorizzate esibiranno alle LRA documentazione analoga a quella indicata al paragrafo precedente.

La LRA verificherà che la persona sia autorizzata ad essere certificata e opererà come indicato nel paragrafo precedente, con l'eccezione del primo punto di tale paragrafo.

F.2.4. Limitazioni d'uso

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di limiti d'uso ovvero di valore per i negozi per i quali può essere usato il certificato stesso, il richiedente deve sottoscrivere idonea documentazione attestante la richiesta. Una copia di tale documentazione viene conservata dal QTSP per 20 (venti) anni.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.2.4.1. Limite d'uso

I certificati possono contenere eventuali limiti d'uso, specificati nell'estensione *certificatePolicies* (*OID:2.5.29.32*) del certificato. In tale estensione è specificato se il certificato è utilizzato in una procedura automatica di firma o sigillo.

Specifici limiti d'uso potranno essere concordati con il Titolare ovvero con il Terzo Interessato.

In particolare: se il certificato sarà utilizzato in procedure di firma automatica, questo dovrà essere specificato nella limitazione d'uso mediante un'asserzione specifica (DPCM, Art. 5, comma 2), ad esempio:

> *"Il presente certificato e' valido solo per firme elettroniche apposte con procedura automatica."*
> *"This certificate may only be used for unattended/automatic electronic signature."*

F.2.5. Abilitazioni professionali e poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di firma elettronica di poteri di rappresentanza (es. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un Cliente, etc.), ovvero di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a dimostrazione dell'effettiva sussistenza di tali abilitazioni professionali. Copia di tale documentazione viene conservata dal QTSP.

La documentazione atta a supportare la richiesta d'inserimento di titoli o abilitazioni professionali all'interno del certificato qualificato non può essere antecedente a 10 (dieci) giorni dalla data di presentazione della richiesta di emissione del suddetto certificato.

L'inserimento nel certificato qualificato d'informazioni relative all'esercizio di funzioni pubbliche o poteri di rappresentanza in enti od organizzazioni di diritto pubblico sarà subordinato a specifici accordi con gli enti stessi. Sulla base di tali accordi sarà possibile specificare il ruolo del Titolare all'interno dell'ente o organizzazione pubblica.

La documentazione prodotta sarà conservata dal QTSP, ovvero dalla LRA incaricata, per un periodo di 20 (venti) anni.

F.2.6. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno Pseudonimo in alternativa ai propri dati reali. In tal caso, lo pseudonimo sarà univocamente assegnato al titolare e le informazioni relative alla reale identità dell'utente saranno conservate per 20 (venti) anni decorrenti dall'emissione del certificato.

F.3. Processo di recepimento della richiesta

Il processo di valutazione della richiesta è svolto dal QTSP tramite la propria RA, ovvero dalla LRA cui sono state demandate le funzioni di Registration Authority.

Nello svolgimento di tale processo, CA, RA/LRA e richiedente/titolare sono vincolati al rispetto degli obblighi di cui al par. *C-Obblighi*.

G. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione

G.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del *Responsabile dei servizi di certificazione e validazione temporale*, come previsto dal DPCM all'Art.7

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

Il tutto avviene in modalità dual control ad evitare operazioni illecite e viene redatto verbale delle operazioni.

Le operazioni successive alla generazione delle coppie di chiavi di certificazione sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto attraverso le chiavi contenute in tali dispositivi di autorizzazione di cui sopra. Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "*n di m*", in modo che solo la concomitante presenza di almeno *n* di *m* parti della chiave permettano di operare con gli opportuni privilegi. Pertanto, esse vengono custodite in apposite casseforti distinte.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

La modalità di sostituzione delle chiavi è descritta al par. *J*.

G.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'art. 49 del DPCM.

L'operazione è svolta in presenza del *Responsabile del servizio di certificazione e validazione temporale* ovvero da persona da questi delegata.

Della chiave pubblica viene generato il certificato, avente validità 10 (dieci) anni, firmato con la chiave privata appositamente generata dal Certificatore.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza dei certificati.

La lunghezza delle chiavi di validazione temporale è conforme alla normativa tempo per tempo vigente.

La modalità di sostituzione delle chiavi è descritta al par. *J*.

G.3. Generazione delle chiavi di sottoscrizione

Completata positivamente la fase di identificazione e registrazione, è possibile procedere alla generazione delle chiavi di firma / sigillo generate dal Certificatore.

Le chiavi di firma / sigillo sono generate su dispositivi di firma che rispondono ai requisiti previsti *dall'Annex II/III* del Reg. eIDAS (*QSCD – Qualified Signature Creation Device*).

In linea generale, per l'emissione di un certificato su di un dispositivo di firma, al netto di identificazioni di tipo unattended (es. SPID, par. F.1.4.1), sono effettuate le seguenti operazioni:

- L'operatore di RA si autentica all'applicazione, seleziona i dati di registrazione del Richiedente e attiva la procedura di richiesta di certificato.

- L'applicazione accede al dispositivo di firma con il PIN di default e genera la coppia di chiavi.
- L'applicazione attivata dall'operatore di RA, dopo la generazione delle chiavi, genera la richiesta di certificato.
- La richiesta viene direttamente inoltrata alla CA; essa è firmata elettronicamente dall'operatore e trasmessa su canale sicuro.
- Il certificato emesso viene ricevuto dall'applicazione e inserito sul dispositivo di firma con le dovute verifiche.
- In caso di Dispositivo Individuale di firma, l'applicazione blocca il PIN di accesso al dispositivo di firma. Al Titolare sarà consegnata, separatamente, una busta contenente il PUK del dispositivo per l'attivazione del medesimo.
- In caso di firma remota, saranno consegnate al Titolare le credenziali di accesso.

La lunghezza delle chiavi di sottoscrizione è conforme alla normativa tempo per tempo vigente.

La modalità di sostituzione delle chiavi è descritta al par. *J*.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel par. *G.1*, sono generati i certificati delle chiavi pubbliche, conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia per l'Italia Digitale attraverso il sistema di comunicazione di cui all'Art.12, comma 1, del DPCM.

Inoltre, il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

Le modalità di sostituzione delle chiavi sono descritte al par. *J*.

H.2. Procedura di emissione dei certificati di validazione temporale

In seguito alla generazione delle chiavi di validazione temporale, descritta al par. *G.2*, vengono generati i certificati delle chiavi pubbliche conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

Della chiave pubblica viene generato il certificato, avente validità 10 (dieci) anni, firmato con la chiave privata appositamente generata dal Certificatore.

L'operazione è svolta in presenza del *Responsabile dei servizi di certificazione* ovvero da persona da questi delegata.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza dei certificati.

Le modalità di sostituzione delle chiavi sono descritte al par. *J*.

H.3. Procedura di emissione dei Certificati di sottoscrizione

Il QTSP INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel par. *G.3*, è generata una richiesta di nuovo certificato nel formato *PKCS#10*, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione della RA / LRA alla Certification Authority del QTSP.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

Il certificato così generato è pubblicato sul registro dei certificati, su richiesta e dietro consenso del Titolare.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

Le modalità di sostituzione delle chiavi sono descritte al par. *J*.

H.3.1. Informazioni contenute nei certificati di sottoscrizione

Il profilo dei certificati qualificati emessi dal QTSP INTESA è conforme al regolamento eIDAS e alle specifiche ETSI di riferimento (par. *S - Riferimenti Tecnici*)

Inoltre, i certificati qualificati emessi in conformità alle *LLGG* riportano la codifica, nel campo *certificatePolicies* (OID 2.5.29.32), di un elemento *PolicyIdentifier* con valore *agIDcert* (OID 1.3.76.16.6). Tutti i certificati qualificati, emessi dalla CA di INTESA in conformità alle LLGG, riportano solo ed esclusivamente il *Key Usage* corrispondente al "*Type A*" della ETSI 319 412-2: *keyUsage (OID 2.5.29.15) = nonRepudiation*.

H.3.2. Accettazione del certificato

I titolari sono tenuti a verificare la correttezza delle informazioni contenute nel certificato loro consegnato e segnalare immediatamente eventuali errori al Certificatore : in tal caso, il Titolare deve sottoscrivere una richiesta di revoca per il certificato contenente dati errati (par. *I - Modalità di revoca e sospensione dei certificati*).

I. Modalità di revoca e sospensione dei certificati

In conformità al Reg. eIDAS, le informazioni sullo stato del certificato sono disponibili via protocollo OCSP, all'URL indicato sul certificato stesso.

La revoca e la sospensione dei certificati possono essere asseverate anche dal loro inserimento nella lista CRL (Art.22 del DPCM). Il profilo delle CRL è conforme con lo standard RFC 3280. Tale lista, firmata dalla Certification Authority emittente il certificato, viene aggiornata con periodicità prestabilita e conforme alla normativa vigente. L'URL della lista CRL è indicato sul certificato, nel campo *CDP - CRL Distribution Point*.

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato (artt. 23, 25, 27 e 29 del DPCM), il Certificatore notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

In fase di richiesta, dovranno essere specificate la data e l'ora a partire dalla quale il certificato dovrà risultare revocato o sospeso e, in questo secondo caso, il periodo di sospensione (Art.24, comma 1, DPCM).

I.1. Revoca dei certificati

Un certificato può essere revocato su richiesta del Titolare, del Terzo Interessato o della Certification Authority (cioè il QTSP).

Il certificato revocato non può essere in alcun modo riattivato.

Un certificato viene revocato nei seguenti casi, ad ognuno dei quali corrisponde un codice detto *CRLReason*:

- *CRLReason* ***Superceded*** sostituzione del certificato senza compromissione della chiave privata;
- *CRLReason* ***Key Compromise***: compromissione (perdita delle caratteristiche di sicurezza e univocità) della chiave privata;
- *CRLReason* ***Affiliation Changed***:i dati del certificato sono obsoleti oppure errati;
- *CRLReason* ***Cessation of Operation***: cessazione preventivata ovvero repentina, in condizioni di conflittualità o no, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati;
- *CRLReason* ***Privilege Withdrawn***: mancato rispetto da parte del Titolare degli obblighi specificati nel CPS o nel Manuale Operativo, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata.

Nota: La causale di revoca *CRLReason* ***Unspecified*** è deprecata.

I.1.1. Revoca su iniziativa del Certificatore

Il QTSP INTESA può revocare i certificati dei titolari nei casi indicati al paragrafo precedente.

In ogni caso informerà dell'avvenuta revoca i titolari interessati tramite posta elettronica, altrimenti tramite posta ordinaria.

I.1.2. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca del proprio certificato secondo tre diverse modalità:

- Qualora il Titolare disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo *uff_ra@intesa.it* contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata. Il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'indirizzo internet *https://www.intesa.it/e-trustcom/*. Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che permettano di identificare univocamente il certificato da revocare - vedi più sotto) e il motivo della richiesta.
- Nei casi in cui il Titolare non disponga di un proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente e allegando un proprio documento di identità:
  - via fax, *al numero indicato all'URL https://www.hda.intesa.it nell'orario di servizio ivi riportato*;
  - via posta ordinaria*, all'indirizzo del QTSP (par. B.2);*
  - eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia la compromissione delle chiave di firma (CRLReason: Key Compromise), il Titolare potrà telefonare al servizio di di helpdesk, fornendo i dati relativi al certificato e il Codice di Emergenza (DPCM, art. 21). In questo caso il certificato indicato sarà temporaneamente sospeso in attesa della richiesta scritta del Titolare.

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'art. 24, comma 1, del DPCM.

Al di fuori degli orari di assistenza indicati all'URL *https://www.hda.intesa.it*, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente, per quanto riguarda il Titolare interessato;

- generalità (es. nome, cognome, e-mail, telefono, ente di riferimento);
- motivazione della richiesta;
- momento di decorrenza del provvedimento.

Altri dati aggiuntivi possono essere utili al fine di identificare univocamente il certificato da revocare. Tali dati possono essere recuperati dal Titolare dalla documentazione rilasciata in fase di emissione, se ancora disponibile (es. tipo di dispositivo e numero seriale, organizzazione di riferimento, numero seriale del certificato, data di rilascio…).

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca al Titolare tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca (CRL).

I.1.3. Revoca su richiesta del Terzo Interessato

Il Terzo Interessato può richiedere la revoca del certificato del Titolare.

Il QTSP INTESA dispone tre diverse modalità per la richiesta di revoca da parte del Terzo Interessato:

- Qualora il Terzo Interessato disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo *uff_ra@intesa.it* contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata (il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'indirizzo internet *https://www.intesa.it/e-trustcom/*. Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che permettano di risalire univocamente al certificato da revocare) e il motivo della richiesta.
- Nei casi in cui il Terzo Interessato non disponga del proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente:
  - via fax, al numero indicato all'URL *https//www.hda.intesa.it/* nell'orario di servizio ivi riportato;
  - via posta ordinaria, all'indirizzo del QTSP (par. *B.2*).

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'art. 25 comma 1 del DPCM.

Al di fuori degli orari di assistenza indicati all'URL *https//www.hda.intesa.it*, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente:

- per quanto riguarda il Terzo Interessato:
  - azienda di appartenenza;
  - generalità;
  - riferimenti al documento che lo autorizza a chiedere l'emissione, la revoca o la sospensione del certificato del Titolare interessato;
  - suoi recapiti: telefonici e di posta elettronica;
- per quanto riguarda il Titolare interessato:
  - generalità;
  - estremi del certificato di cui si chiede la revoca o la sospensione;
  - tipo (revoca o sospensione) e motivazione della richiesta (CRLReason);
  - momento di decorrenza del provvedimento.

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca ai titolari interessati tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca (CRL).

I.2. Sospensione dei certificati

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se il certificato impattato debba essere revocato o no (ad esempio nei casi in cui si tema la compromissione della chiave privata o lo smarrimento/furto del dispositivo di firma, oppure si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

Per una sospensione, il codice di CRLReason è *CRLReason* ***certificateHold***.

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli Artt. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per la richiesta di revoca.

I.2.1.1. Durata del periodo di sospensione

Sarà cura del richiedente comunicare al QTSP, con modalità analoghe a quelle utilizzate per la richiesta di sospensione, la richiesta di riattivazione o di revoca del certificato precedentemente sospeso.

In assenza di comunicazioni, il certificato verrà automaticamente ***revocato*** dopo il periodo di sospensione , indicato dal Titolare nella richiesta e comunque non superiore ai 90 (novanta) giorni, con la *CRLReason* indicata al momento della richiesta stessa.

In caso di revoca di un certificato sospeso, la data di revoca coinciderà con la data di sospensione.

J. Modalità di sostituzione delle chiavi

J.1. Sostituzione delle chiavi del Certificatore

J.1.1. Sostituzione in emergenza delle chiavi di certificazione

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) contenente le chiavi di certificazione (CA e TSCA) o di disastro presso la sede centrale è trattato alla sezione *N - Procedura di gestione degli eventi catastrofici*.

J.1.2. Sostituzione pianificata delle chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alle coppie di Chiavi di certificazione (CA e TSCA), utilizzate dai sistemi di emissione dei certificati di sottoscrizione e dei certificati di TSA, il Certificatore procederà in base a quanto stabilito dall'Art.30 del DPCM.

J.1.3. Sostituzione delle chiavi del sistema di validazione temporale (TSA)

In conformità con quanto indicato all'Art.49, comma 2, del DPCM, ai fini di limitare il numero di marche temporali generate con la medesima coppia di chiavi di validazione temporale, queste sono sostituite entro 90 (novanta) giorni dalla data della loro emissione. Contestualmente, un certificato è emesso relativamente alla nuova coppia di chiavi (senza revocare il precedente, relativo alla coppia di chiavi sostituita).

J.2. Sostituzione delle chiavi del Titolare

I certificati qualificati emessi dal QTSP INTESA hanno una durata standard di 24 / 36 mesi dalla data di emissione, salvo accordi con i singoli clienti e compatibilmente con il loro utilizzo.

Al termine del periodo di validità, si renderà necessaria la generazione di una nuova coppia di chiavi di sottoscrizione e contestualmente l'emissione di un nuovo certificato.

In questo caso la procedura seguita per l'emissione del nuovo certificato sarà simile a quella indicata in fase di primo rilascio, al netto della fase di identificazione del Titolare che non dovrà essere ripetuta se la procedura è effettuata prima della scadenza del certificato.

Entro la data di scadenza del certificato, al Titolare del dispositivo di firma sarà spedito, all'indirizzo di posta elettronica comunicato, un avviso di prossima scadenza.

Il Titolare che intende rinnovare il proprio certificato deve darne comunicazione tempestiva all'Ufficio RA, in modo da garantire la continuità del servizio.

K. Registro dei certificati

K.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

- I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
- I certificati delle chiavi di certificazione (CA e TSCA).
- I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
- I certificati per le chiavi di firma dell'Agenzia per l'Italia Digitale (DPCM Art.42, comma 1).
- Le liste di revoca e sospensione (CRL).

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno; questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

K.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL.

L'accesso sulle copie operative è possibile all'indirizzo *ldap://x500.e-trustcom.intesa.it* con protocollo LDAP.

Il Certificatore consente anche l'accesso alle CRL attraverso il protocollo http, all'URL indicato nel campo CDP (CRL Distribution Point) del certificato.

K.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se in modalità dual control ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

L. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal D.lgs. 196/03 e dal Regolamento Europeo 679/2016 (GDPR) e loro successive modificazioni e integrazioni.

M. Procedura di gestione delle copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *K*.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonché le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del QTSP (Art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

N. Procedura di gestione degli eventi catastrofici

La presenza di sistemi configurati in modalità *dual-site*, con repliche distribuite in più punti consente comunque, in caso di interruzione di funzionamento di una delle sedi, di accedere ai servizi se almeno una delle sedi dei data center è operativa.

Il QTSP INTESA è dotata di un piano di emergenza per la gestione degli eventi catastrofici che prevede le seguenti fasi:

- *gestione dell'emergenza:* attivazione delle soluzioni di *disaster recovery*
- *gestione del transitorio*: servizio attivo e ripristino di ulteriori soluzioni di *disaster recovery*;
- *ritorno dell'esercizio a regime*: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica off-site dei dati e l'intervento entro 24 ore del personale addetto.

O. Modalità per l'apposizione e la definizione del riferimento temporale

Il TSP INTESA offre un servizio qualificato di validazione temporale di documenti elettronici conforme alla normativa vigente.

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata mediante il protocollo *NTP* (*Network Time Protocol*). L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi, a loro volta, sono sincronizzati alla scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (DD/MM/YYYY hh:mm:ss), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM Art.51.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.41 del DPCM).

O.1. Controllo del sincronismo con l'ora campione

I server dedicati ai servizi di marcatura temporale hanno inoltre un controllo software tra l'orario della macchina e un cospicuo numero di server NTP distribuiti a livello planetario: l'utilità di controllo, installata su ognuno dei server utilizzati dal QTSP INTESA nell'ambito della validazione temporale, periodicamente verifica l'allineamento del clock di sistema questi NTP Server di riferimento Se l'allineamento temporale non risulta conforme alle specifiche tecniche di riferimento tempo per tempo vigenti, il servizio di marcatura temporale erogato dallo 00specifico server che risultasse disallineato viene arrestato. Alla data, è previsto il blocco del sistema di validazione temporale in caso di superamento di una soglia di tolleranza fissata a 1 (un) minuto secondo (in valore assoluto).

In caso di blocco, una segnalazione è inviata al personale addetto, al fine di verificarne le cause e intervenire di conseguenza.

O.2. Timestamp token – Marca temporale

Il formato della Marca temporale è conforme con quanto richiesto dal Regolamento eIDAS e, nello specifico, con la *ETSI-319.422*.

O.3. Modalità di richiesta e verifica marche temporali

L'apposizione della marca temporale è solitamente un processo integrato con l'operazione di firma o di sigillatura e non richiede nessuna attività specifica da parte del Titolare.

Anche la verifica della marca temporale apposta è contestuale alla verifica del documento firmato e/o sigillato.

P. Modalità operative per l'utilizzo del sistema di verifica della firma

Come previsto dall'Art.14, comma 1, del DPCM, al fine di effettuare la verifica delle firme digitali, il Certificatore fornisce l'applicazione ***DigitalSign Reader***. Il software è disponibile per il download, assieme alla relativa documentazione, all'URL *https://www.intesa.it/e-trustcom/*.

L'utilizzo del software è gratuito.

L'applicazione permette di verificare qualunque archivio informatico firmato e di visualizzarne il contenuto, qualora la stazione di lavoro sia dotata del software adatto a processare quella tipologia d'archivio. A titolo d'esempio, l'applicazione sarà in grado di visualizzare i documenti caratterizzati dall'estensione ".pdf" qualora sia stata preventivamente installata l'applicazione Acrobat Reader.

La procedura di verifica della firma digitale apposta ad un documento informatico esegue i seguenti controlli:

- verifica della struttura della busta PKCS#7;
- verifica che il certificato del firmatario non sia scaduto;
- verifica che il certificato del firmatario non sia stato revocato o sospeso;
- verifica che il certificato del firmatario sia stato emesso da una Autorità di Certificazione inclusa nell'elenco pubblico dei certificatori accreditati;
- verifica le informazioni presenti nel certificato qualificato, nonché le estensioni obbligatorie (DPCM, Art.14, comma 2b);
- consente l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori accreditati (DPCM, Art.14, comma 2c);
- verifica della validità del certificato di certificazione;
- se presente all'interno del PKCS#7, verifica della marca temporale associata.

Per ulteriori dettagli relativi all'applicazione, si rimanda al manuale utente disponibile sull'applicazione stessa.

Q. Modalità operative per la generazione della firma digitale

Il TSP INTESA mette a disposizione dei propri Clienti strumenti per la generazione della firma digitale sia su documenti singoli che in modalità massiva mediante l'utilizzo di procedure automatiche. Tali strumenti sono conformi a quanto previsto dagli Artt. 4 e 11 del DPCM.

Q.1. Firma mediante dispositivo di firma individuale

Presso il TSP INTESA è possibile acquistare il prodotto ***PKI Smart Kit***. Questa è la soluzione ideale in un kit completo che consente, con facilità d'uso, di eseguire tutte le operazioni relative alla firma digitale: generazione delle chiavi, richiesta di un certificato digitale, sottoscrizione di documento e verifica dello stesso. Grazie a tale tecnologia è possibile apporre la firma digitale a qualunque tipo di documento informatico.

Il package PKI Smart Kit offre una soluzione completa per l'impiego della firma digitale. In particolare, nel kit sono inclusi i seguenti prodotti e servizi:

- identificazione personale dell'utente;
- un dispositivo di firma (smartcard oppure token USB);
- un lettore di smartcard da collegare al PC;
- un certificato qualificato per firma digitale;
- il software di firma ***DigitalSign*** *(par. Q.1.1) o* ***firma4NG*** *(par. Q.1.2)*;
- un CD-ROM contenente:
  - I driver per l'installazione dell'hardware fornito,
  - I manuali d'uso.

La smartcard e il relativo lettore sono forniti in alternativa al token USB.

Il kit è facilmente installabile su un personal computer, sul quale deve essere disponibile una porta di connessione USB.

Q.1.1. Software di firma e verifica – DigitalSign

DigitalSign è l'applicazione fornita dal per la generazione e la verifica di firme digitali e l'apposizione di marche temporali.

Alla prima attivazione, occorre procedere alla configurazione del dispositivo di firma e aggiornare l'elenco dei certificati di CA con le relative CRL. Queste informazioni vengono reperite dalla lista dei Certificati di certificazione tenuta da AgID.

Attivando la funzione di Firma, è richiesto di selezionare il documento da sottoscrivere e di inserire il dispositivo di firma (smartcard ovvero token USB), se non ancora presente. Il documento selezionato viene visualizzato mediante l'applicazione e viene quindi richiesto di digitare il codice PIN del dispositivo di firma. Finalmente, all'utente è richiesto di salvare il documento firmato (*Cades* o *Pades*) e/o marcato temporalmente, se richiesto.

Nel processo di generazione della firma digitale vengono effettuate le seguenti operazioni:

- Verifica che il certificato di sottoscrizione indicato dall'utente non sia scaduto.
- Verifica della corrispondenza tra chiave privata presente sul dispositivo di firma e certificato del Titolare.

L'applicazione *DigitalSign* permette anche l'apposizione di firme multiple allo stesso documento.

Alla firma può associata una marca temporale generata dal servizio di validazione temporale del TSP INTESA, descritto al par. *O - Modalità per l'apposizione e la definizione del riferimento temporale*.

Oltre alle funzioni di generazione di firme, il prodotto offre le seguenti funzionalità:

- Verifica firma: tale funzione è analoga a quella descritta nella sezione P.
- Cifra: tale funzione permette di cifrare un documento, disponendo di un certificato utilizzabile per la cifratura di dati.
- Decifra: tale funzione permette la decifratura di dati precedentemente cifrati.

Per ulteriori dettagli relativi all'applicazione *DigitalSign* si rimanda al manuale utente, disponibile nel prodotto stesso.

Q.1.2. Software di firma e verifica – firma4ng

Il TSP INTESA distribuisce anche il software di firma e verifica ***firma4ng***, un'applicazione professionale di firma digitale, compatibile con i sistemi operativi Windows, Linux e Mac OS X. Permette la firma e la verifica di qualsiasi tipo di documento elettronico.

Per ulteriori dettagli relativi all'applicazione *firma4ng* si rimanda al manuale utente, disponibile nel prodotto stesso

Q.2. Firma con procedure automatiche

Il TSP INTESA offre un servizio di generazione automatica delle firme digitali da utilizzare per la gestione di grossi volumi di documenti. In questo caso i certificati di sottoscrizione generati dal Certificatore risiedono, con le rispettive chiavi private, su di un dispositivo di firma di tipo Hardware Security Module (HSM). Tale metodologia garantisce migliori prestazioni e maggiore sicurezza rispetto ad una smartcard o ad un token USB. Il servizio è conforme a quanto stabilito dalla normativa (DPCM, Art.5, comma 2 e 3) e il formato delle firme elettroniche generate è conforme alla normativa vigente.

Alla firma è associata una marca temporale generata dal servizio di validazione temporale, descritto al par. *O - Modalità per l'apposizione e la definizione del riferimento temporale*.

Q.3. Firma Digitale Remota

Il TSP INTESA offre un servizio Firma Digitale Remota, generata su HSM, conforme alla normativa vigente. Essa è generata su di un HSM custodito e gestito sotto la responsabilità del Certificatore accreditato ovvero dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi. Il Certificatore è in grado, dato un certificato qualificato, di individuare il dispositivo afferente la corrispondente chiave privata

Conformemente alla normativa vigente, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto al par. *O - Modalità per l'apposizione e la definizione del riferimento temporale*.

Q.3.1.1. Dispositivo di Firma Remota presso Terzi

La Firma Remota può essere generata su HSM custoditi e gestiti dall'Organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'Organizzazione che richiede al TSP di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi (Art.3, comma 4 del DPCM)

In questo caso, il TSP deve essere in grado di:

- individuare agevolmente il dispositivo afferente la corrispondente chiave di un dato certificato;
- mettere in essere quanto previsto dall'Art.3, comma 5, del DPCM.

Nel caso in cui il TSP venga a conoscenza dell'inosservanza di quanto ivi esposto, procede alla revoca dei certificati afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.

Q.4. Firma con certificato di validità temporale limitata ("one shot")

Il TSP INTESA offre un servizio Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato a validità temporale limitata (tipicamente 30 minuti dall'emissione o come altrimenti concordato con il cliente / terzo interessato). Essa è generata su di un HSM custodito e gestito sotto la responsabilità del TSP INTESA.

Il Titolare attiva la procedura di firma mediante sistemi di autenticazione consentiti dalla normativa vigente in materia.

Per questa tipologia di certificato, non è prevista la revoca o la sospensione. E' previsto uno specifico limite d'uso, da concordare con il cliente.

Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto al par. *O - Modalità per l'apposizione e la definizione del riferimento temporale*.

Q.5. Autenticazione Biometrica

Il servizio fornito dal TSP INTESA prevede che il Titolare di un certificato di firma digitale possa avviare il processo di firma utilizzando una procedura di riconoscimento *biometrico*.

Perché ciò avvenga, nel rispetto della normativa vigente e garantendo la massima sicurezza della procedura, è previsto che, durante l'identificazione del Titolare, queste nuove tecniche siano utilizzate per registrare dati e parametri specifici del Titolare.

Al momento della firma, al posto dei tradizionali PIN e OTP (*OneTime Password*) solitamente utilizzati in questa tipologia di servizi, al Titolare è richiesto di autenticarsi al servizio utilizzando specifici dispositivi biometrici.

La firma digitale è poi realizzata tramite un sistema di coppie di chiavi asimmetriche, una pubblica e una privata, che consentono al Titolare di rendere manifesta l'autenticità e l'integrità di un documento informatico ad uno o più destinatari che ne possono verificare la validità.

In linea con quanto previsto dall'Art.8 del DPCM, le chiavi di firma sono conservate, su dispositivi HSM.

L'uso esclusivo di tali chiavi, come specificato dall'Art.11, comma 2, del DPCM, è garantito dall'utilizzo del sistema di autenticazione di tipo biometrico.

Per maggiori dettagli, è disponibile un Manuale Operativo dedicato, reperibile all'URL:

https://www.intesa.it/manuali-operativi-e-trustcom/.

Q.6. Formato dei documenti

Le applicazioni fornite dal TSP INTESA permettono l'apposizione della firma digitale su tutti i formati di documenti informatici.

È tuttavia importante sottolineare che alcune tipologie di documento informatico sottoscritti con firma digitale non potrebbero comunque ottenere gli effetti descritti nell'Art.21 del CAD, poiché potrebbero contenere macroistruzioni o codice eseguibile tali da attivare funzionalità che possano modificare gli atti o i dati nello stesso rappresentati.

Nel paragrafo successivo è data una breve descrizione relativa alle principali fonti di macroistruzioni o codice eseguibile.

Q.6.1. Macroistruzioni nei documenti

Attualmente, i prodotti di Office Automation consentono l'uso di procedure automatizzate all'interno dei documenti prodotti (come, ad esempio Macro e /o inserimento di codici di controllo).

A tal proposito, la normativa vigente afferma che l'apposizione della firma digitale su documenti che contengano al loro interno "microistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti previsti per la firma elettronica qualificata.

Oggetti e/o procedure che possono essere presenti all'interno dei documenti sono, a titolo di esempio:

- MACRO: script automatizzati presenti nel documento ed invisibili sul Layout di stampa
- REVISIONI: traccia delle modifiche riportate all'interno del documento
- Script (VBS, JS, ecc.): codici inseriti realizzati tramite linguaggi di alto livello
- Formule e Codici campo, Codici automatici: oggetti specifici che aggiungono funzionalità particolari come, ad esempio, la numerazione automatica delle pagine
- Oggetti e/o link ad essi: parti di documenti differenti da quello preso in considerazione o link a documenti esterni (ad esempio un grafico MS-Excel all'interno di un documento MS-Word).

Si rimanda ai manuali utente degli specifici prodotti per una descrizione dettagliata e aggiornata su come evidenziare le funzionalità di cui sopra e sul come annullarle.

R. Lead Time e Tabella Raci per il rilascio dei certificati

Di seguito si riporta la Tabella relativa al "Lead Time di Processo" per la gestione delle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto	Richiesta	Ente Coinvolto	Azione Ente Coinvolto	Ente Coinvolto	Azione Ente Coinvolto
Utente, Richiedente, Titolare Certificato	*Richiesta di Emissione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Azienda (acting as LRA)*	*Emette ordine di pubblicazione del Certificato vs CA previa verifica identità*	*Intesa (acting as) Certification Authority*	*Evasione Richiesta di Certificazione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Revoca / Sospensione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Azienda (acting as LRA)*	*Emette ordine di Revoca / Sospensione del Certificato vs CA previa verifica identità*	*Intesa (acting as) Certification Authority*	*Evasione Richiesta di Revoca / Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Azienda (acting as LRA)*	*Emette ordine di riattivazione del Certificato vs CA previa verifica identità*	*Intesa (acting as) Certification Authority y*	*Evasione Richiesta di Riattivazione*

Di seguito si riporta la Tabella RACI relativa alla individuazione delle responsabilità degli enti coinvolti nelle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto Coinvolto	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Utente, Richiedente, Titolare del Certificato			***X***	***X***

S. Riferimenti Tecnici

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-3	ETSI EN 319 412-3 V1.2.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to legal persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)

------- FINE DEL DOCUMENTO -------